

Detection of entanglement in asymmetric quantum networks and multipartite quantum steering

D. Cavalcanti,^{1,*} P. Skrzypczyk,¹ G. H. Aguilar,² R. V. Nery,² P. H. Souto Ribeiro,² and S. P. Walborn²

¹*ICFO-Institut de Ciències Fotoniques, Mediterranean Technology Park, 08860 Castelldefels (Barcelona), Spain*

²*Instituto de Física, Universidade Federal do Rio de Janeiro, CP 68528, 21941-972, Rio de Janeiro, RJ, Brazil*

The future of quantum communication relies on quantum networks composed by observers sharing multipartite quantum states. The certification of multipartite entanglement will be crucial to the usefulness of these networks. In many real situations it is natural to assume that some observers are more trusted than others in the sense that they have more knowledge of their measurement apparatuses. Here we propose a general method to certify all kinds of multipartite entanglement in this asymmetric scenario and experimentally demonstrate it in an optical experiment. Our results, which can be seen as a definition of genuine multipartite quantum steering, gives a method to detect entanglement in a scenario in-between the standard entanglement and fully device-independent scenarios, and provides a basis for semi-device-independent cryptographic applications in quantum networks.

I. INTRODUCTION

The most widely used techniques to detect entanglement rely either on having knowledge of the quantum state, obtained through quantum state tomography, or on the use of measurements that constitute an entanglement witness [58]. A frequently disregarded assumption behind these methods is that the measurements and devices used are well characterized. However, a mismatch between the theoretical description of the measurements and their actual implementation may lead to erroneous conclusions about the presence of entanglement [2]. A way of avoiding this assumption is to use device-independent techniques [50], where the measuring devices are not trusted to behave as expected, and no specific description of the experimental observables is assumed. In this approach the measurement devices are considered as black boxes that the parties can access with classical inputs (corresponding to the measurement choices) that provide classical outputs (considered as the measurement results). The presence of entanglement is then verified analyzing the correlation statistics between the data lists corresponding to the measurement results. The violation of Bell inequalities [4] certify the presence of entanglement in this scenario, which can be thought of as a device-independent entanglement witness. The device-independent approach is especially important in adversarial scenarios, such as device-independent quantum key distribution [5], where an adversary can use a mismatch between the real implementation of the protocol and its description to fake its performance [6–8]. However, the violation of a Bell inequality requires a high degree of correlation between the parties tolerating then very low levels of noise and demanding highly efficient detectors and high-quality entangled states [50].

An intermediate scenario between the standard and the device-independent cases is that of quantum steering [9, 49]. This is the situation where, in the bipartite case, one of the parties uses a trusted measuring device but the other does not. As such, we refer to this approach as the semi-device-

independent one. Apart from the fundamental importance of characterizing separability in different scenarios, quantum steering appears as a practical situation that is less demanding experimentally than the device-independent approach. It requires fewer assumptions than the standard case and lower strength for the quantum correlations to be witnessed or certified. For these reasons the study of quantum steering, including its applications [11, 12] and experimental demonstrations [13–19], have increased rapidly over recent years.

In the multipartite case, much knowledge has been acquired concerning standard entanglement detection [58] and the device-independent case [20–22, 24–27, 48]. However, only few results were found in the semi-device-independent case. For instance, Ref. [28] provides inequalities to rule out fully separable states, Ref. [29] developed a probabilistic protocol to detect the presence of a particular multipartite entangled state, and Ref. [30] discussed a hybrid model where each party is sometimes trusted and sometimes untrusted (see also [31, 32] for recent experimental demonstrations).

Apart from the fundamental problem of understanding multipartite quantum correlations, extending the semi-device-independent approach to the multipartite scenario is also relevant for practical purposes. As technology advances it will be possible to establish large quantum networks. These networks will be asymmetric in many cases, depending on the experimental capabilities of each station, the specific architecture of the implemented protocols, and unavoidable limitations that the setup may impose. Let us give few examples. Consider for instance prepare-and-measure cryptographic protocols in which some parties hold the sources of quantum systems and some others act as the receivers who measure these systems. Since the senders do not receive any external signals they may consider that no eavesdropper is manipulating their apparatuses. Thus, any error they observe (as for example due to detection inefficiencies) can be attributed to the apparatuses' imperfections. The receivers, on the other hand, are given systems that may have been intercepted by an eavesdropper, who may use extra degrees of freedom that are not considered by the receiver (see [6–8] for examples). In this case, the receivers' apparatuses can not be considered trusted. Another scenario is that in which no reference frame can be established by some of the stations [33]. In this case, the measurement di-

*Electronic address: daniel.cavalcanti@icfo.es

reactions that some of parties implement are not known, and may as well be considered as untrusted. Finally, quantum-key-distribution systems and quantum randomness generators are nowadays at the commercial level. Clearly, the general consumers of these products are not capable of reverse engineering the devices, and may not want to trust their providers.

Here we propose a general method to detect all kinds of entanglement that can be present in a quantum network, where some of the parties use untrusted measurements and must use data lists. We show how the different types of entanglement constrain the corresponding observed experimental data and present an efficient method to obtain semi-device-independent entanglement witnesses in the form of multipartite steering inequalities. We furthermore implement this method in a proof-of-principle optical experiment and demonstrate the violation of multipartite steering inequalities in both scenarios where either one or two parties perform untrusted measurements. Finally, we also quantify the advantage that the present approach provides over the device-independent one in terms of tolerance to noise.

II. RESULTS

A. Semi-device-independent test of multipartite entanglement

We start by explaining the scenario considered here, which consists of a quantum network on N parties sharing an unknown system in state ρ (see Fig. 1). Some of the parties perform measurements that are uncharacterised, or untrusted, while others have total control over their measurement apparatuses. Those parties who do not trust their apparatuses treat them as black boxes in which they can provide classical inputs (corresponding to the choice of measurement settings) and receive classical outputs (corresponding to the measurement outcomes). Notice that not even the Hilbert space dimension of these systems are assumed. The parties that trust their measurements can actually implement quantum state tomography, and reconstruct the density matrix they hold after the untrusted parties announce their measurement choices and outcomes. Based on this knowledge the goal is to decide if the original state ρ had some kind of entanglement.

In the general case of N parties there will be several semi-device-independent cases, depending on which parties are trusted. For simplicity, in what follows we will explain our method for the case of detecting genuine multipartite entanglement in a tripartite system. This case contains all the basic ingredients needed to understand both how to detect other types of entanglement and how to treat systems composed of more parties. These procedures are described in detail in the Supplementary Notes I-III.

Let us consider that an unknown tripartite state ρ^{ABC} is distributed between three parties: Alice, Bob and Charlie. Two semi-device-independent cases arise: (i) when only one party's device is untrusted and (ii) when two parties' devices are untrusted. Let us consider the first case, supposing that Alice holds the untrusted device. In this case, there is no assumptions on Alice's measurements and we describe them

with some unknown measurement operators $M_{a|x}$, where the subscript x labels the measurement choices and a the possible outcomes. Not even the dimension of Alice's subsystem is assumed. Since Bob and Charlie trust their apparatuses they can perform tomography and determine their (unnormalized) conditional states $\sigma_{a|x}^{BC}$ as

$$\sigma_{a|x}^{BC} = \text{tr}_A(M_{a|x} \otimes \mathbb{1}_B \otimes \mathbb{1}_C \rho^{ABC}). \quad (1)$$

The set of unnormalized states $\{\sigma_{a|x}^{BC}\}_{a,x}$ is called an assemblage and contains all the information obtainable in this situation as it encodes both the probability that Alice obtains the result a given that she made the measurement x , as $p(a|x) = \text{tr}(\sigma_{a|x}^{BC})$, as well as the corresponding conditional state $\rho_{a|x}^{BC} = \sigma_{a|x}^{BC}/p(a|x)$.

The second situation is when two parties, say Alice and Bob, have untrusted devices. In this situation Bob's measurement is also treated as a black box performing measurements associated to unknown measurement operators $M_{b|y}$, while Charlie can tomographically determine the assemblage

$$\sigma_{ab|xy}^C = \text{tr}_{AB}(M_{a|x} \otimes M_{b|y} \otimes \mathbb{1}_C \rho^{ABC}). \quad (2)$$

The probability distributions of Alice and Bob's measurements is encoded in $p(ab|xy) = \text{tr} \sigma_{ab|xy}^C$.

If the initial state ρ^{ABC} contains no genuine multipartite entanglement, *i.e.* it is biseparable, then it has the form

$$\begin{aligned} \rho^{ABC} = & \sum_{\lambda} p_{\lambda}^{A:BC} \rho_{\lambda}^A \otimes \rho_{\lambda}^{BC} + \sum_{\mu} p_{\mu}^{B:AC} \rho_{\mu}^B \otimes \rho_{\mu}^{AC} \\ & + \sum_{\nu} p_{\nu}^{AB:C} \rho_{\nu}^{AB} \otimes \rho_{\nu}^C, \end{aligned} \quad (3)$$

where $p_{\lambda}^{A:BC}$, $p_{\mu}^{B:AC}$ and $p_{\nu}^{AB:C}$ are probability distributions. Then the assemblages (1) and (2) have the form

$$\begin{aligned} \sigma_{a|x}^{BC} = & \text{tr}(M_{a|x} \otimes \mathbb{1}_B \otimes \mathbb{1}_C \rho^{ABC}) \\ = & \sum_{\lambda} p_{\lambda}^{A:BC} p_{\lambda}(a|x) \rho_{\lambda}^{BC} \end{aligned} \quad (4)$$

$$+ \sum_{\mu} p_{\mu}^{B:AC} \rho_{\mu}^B \otimes \sigma_{a|x,\mu}^C \quad (5)$$

$$+ \sum_{\nu} p_{\nu}^{AB:C} \sigma_{a|x\nu}^B \otimes \rho_{\nu}^C \quad (6)$$

and

$$\begin{aligned} \sigma_{ab|xy}^C = & \text{tr}_{AB}(M_{a|x} \otimes M_{b|y} \otimes \mathbb{1}_C \rho^{ABC}) \\ = & \sum_{\lambda} p_{\lambda}^{A:BC} p_{\lambda}(a|x) \sigma_{b|y,\lambda}^C \end{aligned} \quad (7)$$

$$+ \sum_{\mu} p_{\mu}^{B:AC} p_{\mu}(b|y) \sigma_{a|x,\mu}^C \quad (8)$$

$$+ \sum_{\nu} p_{\nu}^{AB:C} p_{\nu}(ab|xy) \rho_{\nu}^C \quad (9)$$

respectively.

Thus, the fact that the original state is biseparable imposes constraints on the observed assemblages. For instance, in (4) the dependence on the variables a and x is only through the distribution $p_{\lambda}(a|x)$ and not through the quantum states. This is a typical instance of an unsteerable bipartite assemblage [49]. The assemblage in (5) satisfies two constraints: each conditional state is a separable state, and the dependence in a and x is due only to Charlie's system, and not Bob's. The assemblage in (6) is similar to the one in (5), only with Bob's and Charlie's roles exchanged. Thus, in order to test if a given assemblage $\sigma_{a|x}^{obs}$ has the form (4) consistent with having been produced by a biseparable state one could run the following program:

$$\begin{aligned} & \text{find } \Gamma_{a|x}^{A:BC}, \Gamma_{a|x}^{B:AC}, \Gamma_{a|x}^{C:AB}, \\ & \text{such that} \\ & \sigma_{a|x}^{obs} = \Gamma_{a|x}^{A:BC} + \Gamma_{a|x}^{B:AC} + \Gamma_{a|x}^{C:AB}, \\ & \Gamma_{a|x}^{A:BC} \geq 0, \Gamma_{a|x}^{B:AC} \geq 0, \Gamma_{a|x}^{C:AB} \geq 0, \\ & \Gamma_{a|x}^{A:BC} \text{ is unsteerable,} \\ & \Gamma_{a|x}^{B:AC} \text{ is separable and unsteerable from } A \text{ to } B, \\ & \Gamma_{a|x}^{C:AB} \text{ is separable and unsteerable from } A \text{ to } C. \end{aligned} \quad (10)$$

If no such triple of assemblages exists, then the underlying state was definitely not biseparable, and therefore genuine multipartite entangled. The main problem with this method is that, apart from systems with dimension lower than 6, testing separability is computationally demanding [34]. As we show in the Supplementary Notes I and II, we can overcome this problem by considering approximations of the set of separable states which relax the above program into a semidefinite program (SDP) [53, 54], for which efficient numerical methods exist.

A similar analysis can be made for the decomposition (7) (see Supplementary Note II) and other types of entanglement (see Supplementary Table I). For instance, (7) refers to an assemblage that is unsteerable from A to C and (8) to one that is unsteerable from B to C . The assemblage (9) has two properties: it is unsteerable, and the probability distributions $p_{\nu}(ab|xy)$ must have quantum realisations, *i.e.* must come from measurements on quantum states. Again, this last requirement is in general difficult to test. However, we can once again make use of relaxations of the set of quantum probability distributions [57] to transform the program into a semidefinite program.

All in all, for each semi-device-independent scenario the type of entanglement in the distributed state will impose constraints on the assemblages one could observe. These constraints allow the parties holding the trusted devices to determine if this state must have been genuine multipartite entangled (*e.g.* if the observed data admits no decomposition of the form (4) or (7) then there exists no biseparable state that could explain it). Therefore, even not knowing the initial state or what type of measurements the untrusted parties performed, it is possible to discriminate the assemblages that were produced by states containing some type of entanglement.

Finally, in each case the program can be seen as a membership test for the observed assemblage to be contained in-

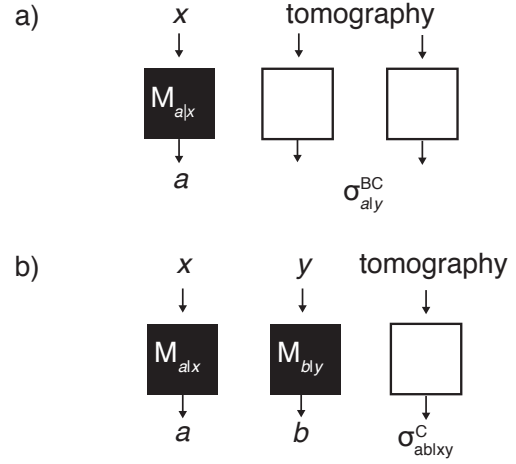


FIG. 1: Asymmetric tripartite networks where untrusted devices are treated as black boxes with classical inputs and outputs a) One untrusted party scenario: Alice, who holds an untrusted device treats it as a black box in which she inputs x (the measurement choice) and receives an output a (the measurement outcome). This procedure corresponds mathematically to applying some unknown measurement operator $M_{a|x}$ to the shared tripartite quantum state, which produces a post-measured state $\sigma_{a|x}^{BC}$ at Bob and Charlie's locations. b) A similar situation occurs in two untrusted parties scenario, when both Alice and Bob perform untrusted measurements (corresponding to unknown measurement operators $M_{a|x}$ and $M_{b|y}$ respectively) preparing quantum states $\sigma_{ab|xy}^C$ on Charlie's system.

side a convex set. It is always possible to certify that a point lies outside a convex set by finding a separating hyperplane between the set and the point. As we show in the Supplementary Note II, in each case we can find the lagrange dual program to the set membership test, which always amounts to finding such a separating hyperplane. Such separating hyperplanes are precisely multipartite steering inequalities, which can alternatively be thought of as semi-device independent entanglement witnesses. Thus our method naturally generates steering inequalities which can then be used as witnesses for multipartite entanglement.

B. Practical considerations

Due to experimental errors and finite statistics the experimentally observed data is not strictly compatible with any physical state and local measurements. In particular, all assemblages which exactly reproduce the experimental data in general do not satisfy the no-signalling constraint that $\sum_a \sigma_{a|x}^{BC} = \sum_a \sigma_{a|x'}^{BC}$ for $x \neq x'$. Since the present methods are tailored to detect entanglement of physical states we can not use the observed data directly to test for the presence of entanglement.

We thus propose to proceed with the following steps: First, given the experimental data, generate a physical assemblage that best approximates it through, for instance, a maximum likelihood reconstruction method. Second, having obtained

the best physical approximation to the actual data, use the SDP method discussed in the Supplementary Note II to check for any type of entanglement. This method also generates an inequality that is satisfied by all assemblages coming from states which do not have the type of entanglement tested. Finally check that the observed data violates this inequality.

C. Examples: GHZ and W states

As examples, we used our method to produce the following inequality that is satisfied by all assemblages of the form (1) (see also Supplementary IV):

$$1 + 0.1547\langle Z_B Z_C \rangle - \frac{1}{3}(\langle A_3 Z_B \rangle + \langle A_3 Z_C \rangle + \langle A_1 X_B X_C \rangle - \langle A_1 Y_B Y_C \rangle - \langle A_2 X_B Y_C \rangle - \langle A_2 Y_B X_C \rangle) \geq 0, \quad (11)$$

with A_i for $i = 1, 2, 3$, being observables in Alice's system with outcomes labelled ± 1 and X, Y and Z representing the Pauli operators. The GHZ state $(|000\rangle + |111\rangle)/\sqrt{2}$ violates this inequality by $-0.8453 \not\geq 0$ when Alice's measurements are also X, Y and Z , which numerical optimization suggests are the optimal choices for Alice.

In the case Alice and Bob perform untrusted measurements we have derived the following inequality which is satisfied by assemblages of the form (2):

$$1 - \alpha\langle A_3 B_3 \rangle - \alpha\langle A_3 Z \rangle - \alpha\langle B_3 Z \rangle - \beta\langle A_1 B_1 X \rangle + \beta\langle A_1 B_2 Y \rangle + \beta\langle A_2 B_1 Y \rangle + \beta\langle A_2 B_2 X \rangle \geq 0 \quad (12)$$

where $\alpha = 0.1831$ and $\beta = 0.2582$, and similarly B_i for $i = 1, 2, 3$ represent Bob's measurement which we assume to have ± 1 outcomes. The GHZ state achieves a violation $-0.5820 \not\geq 0$ now when both Alice and Bob perform X, Y and Z measurements.

Similar inequalities for two untrusted parties and for the W state, given by $|W\rangle = (|001\rangle + |010\rangle + |100\rangle)/\sqrt{3}$, are presented in the Supplementary Note IV.

We have also considered noisy versions of the GHZ and W states given by

$$\rho_\psi = w|\psi\rangle\langle\psi| + (1-w)\mathbb{1}/8, \quad (13)$$

where $|\psi\rangle$ can be either the GHZ or the W state. We computed how much white noise can be added to these states until we are unable to detect genuine multipartite entanglement. Specifically, we quantify the minimum w for which our method guarantees that following states are genuinely multipartite entangled. The results are summarized in Table III, together with the known bounds for standard entanglement tests [44, 46] and the device-independent case [48]. One can see that trusting some of the parties offers a significant advantage in terms of noise tolerance.

D. Experimental violation of genuine tripartite steering witnesses

In order to illustrate the utility and efficiency of our approach, we use this technique to violate genuine multipartite

steering witnesses in a real laboratory setting where one or two parties perform untrusted measurements. The experimental set-up is shown in Fig 2 and is set to produce a GHZ state encoded in the polarization and path degree of freedom of two photons [40, 41] with high fidelity. The experimental procedure starts preparing photons in a state close to

$$|\Psi\rangle = \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}} \right)_{A_p B_p} \otimes |0\rangle_{B_s}, \quad (14)$$

where A_p and B_p represent the polarization qubit of photons A and B respectively, where 0 and 1 stand for horizontal and vertical polarization states, and B_s represents the spatial degree of freedom of photon B. To obtain a GHZ state, we couple the spatial degree of freedom with the polarization using Beam Displacer (BD1) which transforms $|0\rangle_{B_p}|0\rangle_{B_s} \rightarrow |0\rangle_{B_p}|0\rangle_{B_s}$ and $|1\rangle_{B_p}|0\rangle_{B_s} \rightarrow |1\rangle_{B_p}|1\rangle_{B_s}$. Once we obtain the desired state, every qubit is measured in the eigenstates of the three Pauli operators. For the polarization degrees of freedom this is carried out using a quarter-wave-plate (QWP), a half-wave plate (HWP) and a polarizing beam splitter (PBS) or BD2, depending on the photon. For the spatial degrees of freedom this is carried out using the interferometer described in Fig. 2 [40, 41].

Although this experiment is tailored to produce a GHZ state and perform measurements corresponding to the Pauli operators, the analysis we perform on the experimental data makes no assumption about the state nor the untrusted measurements. We consider two cases, one where part A_p is untrusted and parts B_p and B_s hold the trusted devices, and another when parts B_p and B_s hold the untrusted devices and part A_p the trusted one. For the two cases we follow the procedure described in Sec. II B (using a least-squares optimisation to provide physical assemblages), which provides inequalities of the form $S \geq 0$ (whose exact form can be found in the Supplementary Note V) whose violation certify that the corresponding assemblages cannot be written in the biseparable form (4) or (7), respectively. We finally observe a violation of these inequalities by the experimental data (see Fig. 2 b)). We have performed each experiment (*i.e.* measuring all correlators) 215 independent times, from which we calculate an average value of $S = -0.82 \pm 0.05$ for one untrusted party and $S = -0.56 \pm 0.04$ for two untrusted parties. This proves that there exists no biseparable tripartite state and measurements performed by the untrusted parties that could have generated the observed assemblages.

III. DISCUSSION

We have derived a method to detect multipartite entanglement when some of the apparatuses used in a quantum network are untrusted or uncharacterized. This method allows the detection of all kinds of entanglement in quantum networks where some of the observers use their measurement apparatuses simply as data lists. This scenario is experimentally less demanding than the nonlocality scenario, as it tolerates more noise, for instance. We have performed a proof-of-principle experiment demonstrating the existence of genuine

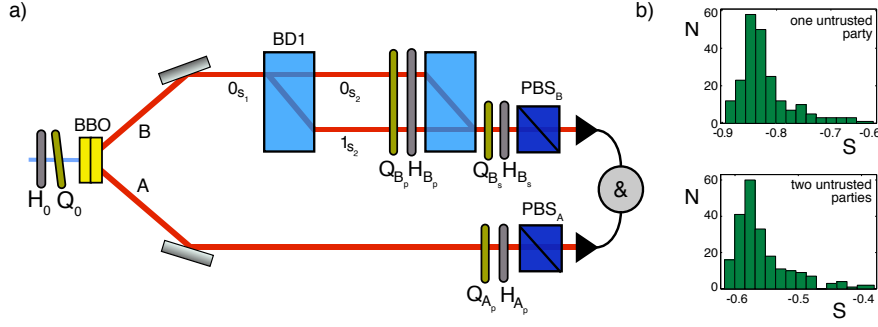


FIG. 2: **Experimental setup and results** a) An ultraviolet laser oscillating at 325nm pumps two cross axis BBO crystals, each 1mm long. Probabilistically, two photons are produced in the state (14) via parametric down conversion [42]. The polarization entangled state is obtained by the superposition of signal and idler beams produced in the first crystal with vertical polarization and the ones produced in the second crystal with horizontal polarization. Signal photons in B are sent to beam displacer BD1 which transmits the vertical polarization component and deviates the horizontally polarized component. This results in the production of a GHZ state right after BD1. Two qubits in this state are represented by the polarization degrees of freedom of photons A and B, and one qubit is encoded in the spatial (or path) degree of freedom of photon B. Photons in mode A are sent directly to detection after polarization projection, which is done using the quarter waveplate Q_{A_p} , half waveplate H_{A_p} , and polarizing beam splitter PBS_A . We perform a joint analysis of the polarization and path degree of freedom of photon B using the sequence of devices given by quarter waveplate Q_{B_p} , half waveplate H_{B_p} , beam displacer BD2, quarter waveplate Q_{B_s} , half waveplate H_{B_s} , and polarizing beam splitter PBS_B . For a given set of adjustments of the quarter and half waveplates, we perform one specific joint projection in both polarization and path degrees of freedom basis. Since there is a coherent combination of spatial modes 0 and 1 in BD2, the measure of the spatial degrees of freedom of photon B is done by mapping the spatial qubit state before BD2 in the polarization state at the output of BD2. Even though the projection is made simultaneously for both degrees of freedom in this case, they are independent, or in other words, all combinations of projections are possible [40, 41]. b) Histograms obtained by computing the semi-device-independent entanglement witness from the experimental data (see main text and the Supplementary Note V for more details about the witness). We measured the value of each witness 215 independent times and plot the number of times N the value S of the witness felt within a given interval. From this statistical procedure, an average value and a variance is obtained for the witness. The upper histogram is for the case of one untrusted party, resulting in the average value of -0.82 and standard deviation of 0.05. The lower histogram is for the case of two untrusted parties, resulting in the average of -0.56 and an standard deviation of 0.04.

tripartite entanglement, without any assumption on the source or the measurements being performed in some of the subsystems.

Our results provide a feasible test for multipartite entanglement in quantum networks and bridges the two well known cases of multipartite entanglement and multipartite Bell non-locality. Moreover the scenario considered is a natural generalization of bipartite quantum steering [49] (see [28, 30] for alternative definitions). Since steering has found applications in cryptographic protocols [11, 12], we believe that our results can be used as a starting point to define semi-device-independent cryptographic applications in future quantum networks.

IV. ACKNOWLEDGEMENTS

We thank A. Acín, M. Navascués and L. Aolita for discussions. DC was supported by the Beatriu de Pinós fellowship (BP-DGR 2013) and PS by the Marie Curie COFUND action through the ICFOnest program. Financial support was provided by Brazilian agencies FAPERJ, CNPq, CAPES, and the National Institute of Science and Technology for Quantum Information.

no. untr. meas.	0	1	2	3
GHZ	$\frac{3}{7} \approx 0.429$	≈ 0.54	≈ 0.63	$2/3 \approx 0.67$
W	≈ 0.479	≈ 0.57	≈ 0.67	≈ 0.72

TABLE I: Critical robustness to white noise w . We provide a comparison between the known bounds on critical robustness to white noise of the GHZ and W states above which genuine multipartite entanglement can be detected in 4 different scenarios: when no party is untrusted (*i.e.* the standard entanglement scenario [44, 46]), when 1 and 2 parties hold untrusted devices, for which we used the semi-device-independent method developed here and when all devices are untrusted, *i.e.* the device-independent case developed in [48]. In the Supplementary Table II we also display the bounds concerning the detection of (not necessarily genuine multipartite) entanglement in these states.

Supplementary note 1

Characterising multipartite assemblages

Here we determine the constraints that different types of entanglement in the initial state ρ^{ABC} impose on the assemblages produced by untrusted measurements and define the corresponding sets that they characterise. We will first consider the question of whether or not there is any entanglement in the state, before moving on to entanglement in a given

Form of state	Untrusted parties	Known objects	SDP
$\sum_{\lambda} p_{\lambda} \rho_{\lambda}^A \otimes \rho_{\lambda}^B \otimes \rho_{\lambda}^C$	A	$\sigma_{a x}^{BC}$	$\begin{aligned} \max \quad & p \\ \text{s.t.} \quad & \sum_{\mu} D_{\mu}(a x) \sigma_{\mu}^{BC} = \sigma_{a x}^{BC} - p \text{id}_{a x}^{BC}, \\ & \left(\sigma_{\mu}^{BC} \right)^{TB} \geq 0, \quad \sigma_{\mu}^{BC} \geq 0. \end{aligned} \quad (15)$
	A and B	$\sigma_{ab xy}^C$	$\begin{aligned} \max \quad & p \\ \text{s.t.} \quad & \sum_{\mu, \lambda} D_{\mu}(a x) D_{\lambda}(b y) \sigma_{\mu\lambda}^C = \sigma_{ab xy}^C - p \text{id}_{ab xy}^C, \\ & \sigma_{\mu\lambda}^C \geq 0. \end{aligned} \quad (16)$
$\sum_{\lambda} p_{\lambda} \rho_{\lambda}^A \otimes \rho_{\lambda}^{BC}$	A	$\sigma_{a x}^{BC}$	$\begin{aligned} \max \quad & p \\ \text{s.t.} \quad & \sum_{\mu} D_{\mu}(a x) \sigma_{\mu}^{BC} = \sigma_{a x}^{BC} - p \text{id}_{a x}^{BC}, \\ & \sigma_{\mu}^{BC} \geq 0. \end{aligned} \quad (17)$
	B	$\sigma_{b y}^{AC}$	$\begin{aligned} \max \quad & p \\ \text{s.t.} \quad & \Gamma_{b y}^{AC} = \sigma_{b y}^{AC} - p \text{id}_{b y}^{AC}, \\ & \text{tr}_C \Gamma_{b y}^{AC} = \sum_{\mu} D_{\mu}(b y) \sigma_{\mu}^A, \\ & (\Gamma_{b y}^{AC})^{TA} \geq 0, \quad \Gamma_{b y}^{AC} \geq 0, \quad \sigma_{\mu}^A \geq 0. \end{aligned} \quad (18)$
	A and B	$\sigma_{ab xy}^C$	$\begin{aligned} \max \quad & p \\ \text{s.t.} \quad & \sum_{\mu} D_{\mu}(a x) \sigma_{b y, \mu}^C = \sigma_{ab xy}^C - p \text{id}_{ab xy}^C, \\ & \sigma_{b y, \mu}^C \geq 0. \end{aligned} \quad (19)$
	B and C	$\sigma_{bc yz}^A$	$\begin{aligned} \max \quad & p \\ \text{s.t.} \quad & \sum_{\mu} D^{\text{NS}}(bc yz, \mu) \sigma_{\mu}^A = \sigma_{bc yz}^A - p \text{id}_{bc yz}^A \\ & \sum_{\mu} D^{\text{NS}}(bc yz, \mu) \sigma_{\mu}^A \in \mathcal{Q}_A^{(k)}, \quad \sigma_{\mu}^A \geq 0 \end{aligned} \quad (20)$
$\begin{aligned} & \sum_{\lambda} p_{\lambda}^{A:BC} \rho_{\lambda}^A \otimes \rho_{\lambda}^{BC} \\ & + \sum_{\lambda} p_{\lambda}^{B:AC} \rho_{\lambda}^B \otimes \rho_{\lambda}^{AC} \\ & + \sum_{\lambda} p_{\lambda}^{AB:C} \rho_{\lambda}^{AB} \otimes \rho_{\lambda}^C \end{aligned}$	A	$\sigma_{a x}^{BC}$	$\begin{aligned} \max \quad & p \\ \text{s.t.} \quad & \Gamma_{a x}^{A:BC} + \Gamma_{a x}^{B:AC} + \Gamma_{a x}^{C:AB} = \sigma_{a x}^{BC} - p \text{id}_{a x}^{BC} \\ & \Gamma_{a x}^{A:BC} = \sum_{\mu} D_{\mu}(a x) \sigma_{\mu}^{BC}, \quad \sigma_{\mu}^{BC} \geq 0 \\ & \text{tr}_C \Gamma_{a x}^{B:AC} = \sum_{\mu} D_{\mu}(a x) \sigma_{\mu}^B, \quad \sigma_{\mu}^B \geq 0, \\ & \text{tr}_B \Gamma_{a x}^{C:AB} = \sum_{\mu} D_{\mu}(a x) \sigma_{\mu}^C, \quad \sigma_{\mu}^C \geq 0, \\ & \left(\Gamma_{a x}^{B:AC} \right)^{TB} \geq 0, \quad \left(\Gamma_{a x}^{C:AB} \right)^{TB} \geq 0. \\ & \Gamma_{a x}^{B:AC} \geq 0, \quad \Gamma_{a x}^{C:AB} \geq 0, \quad \sum_a \Gamma_{a x}^{B:AC} = \sum_a \Gamma_{a x'}^{B:AC}. \end{aligned} \quad (21)$
	A and B	$\sigma_{ab xy}^C$	$\begin{aligned} \max \quad & p \\ \text{s.t.} \quad & \Pi_{ab xy}^{A:BC} + \Pi_{ab xy}^{B:AC} + \Pi_{ab xy}^{C:AB} = \sigma_{ab xy}^C - p \text{id}_{ab xy}^C \\ & \Pi_{ab xy}^{A:BC} = \sum_{\mu} D_{\mu}(a x) \sigma_{b y, \mu}^C, \quad \sigma_{b y, \mu}^C \geq 0 \\ & \Pi_{ab xy}^{B:AC} = \sum_{\mu} D_{\mu}(b y) \sigma_{a x, \mu}^C, \quad \sigma_{a x, \mu}^C \geq 0 \\ & \Pi_{ab xy}^{C:AB} = \sum_{\nu} D_{\nu}^{\text{NS}}(ab xy) \sigma_{\nu}^C, \quad \sigma_{\nu}^C \geq 0 \\ & \Pi_{ab xy}^{C:AB} \in \mathcal{Q}_C^{(k)}, \quad \sum_b \sigma_{b y, \mu}^C = \sum_b \sigma_{b y', \mu}^C \end{aligned} \quad (22)$

TABLE II: **Collection of all SDP tests for the tripartite case.** All expressions with indices should be understood to hold for each value of the index. Various SDPs depend upon a parameter k , such that for larger values of k we obtain a better approximate characterisation of the set, and therefore a more stringent test. All programs are strictly feasible and are such that a negative optimal value $p^* < 0$ certifies that the assemblage has the corresponding type of entanglement. In this case the dual provides a semi-device-independent entanglement witness in the form of a steering inequality. An optimal solution $p^* \geq 0$ indicates that the assemblage is inside the corresponding set, i.e. that one cannot conclude that the state contains the desired type of entanglement.

no. untr. no. meas.		EW 0 n/a	SW 1		SW 2		DIEW 3	
			2	3	2	3	2	3
GHZ	ent.	$\frac{1}{5} = 0.2$ [43]	≈ 0.2613	≈ 0.2500	$\frac{1}{2} = 0.5$	$\frac{3}{7} \approx 0.4286$	$\frac{1}{2} = 0.5$ [47]	$\frac{1}{2} = 0.5$ [47]
	GME	$\frac{3}{7} \approx 0.4286$ [44]	≈ 0.6307	≈ 0.5420	$\frac{1}{\sqrt{2}} \approx 0.7071$	≈ 0.6322	$\frac{1}{\sqrt{2}} \approx 0.7071$ [48]	$\frac{2}{3} \approx 0.6667$ [48]
W	ent.	≈ 0.2096 [45]	$\frac{3}{11} \approx 0.2727$	≈ 0.2698	≈ 0.5765	≈ 0.4434	≈ 0.6442 [47]	≈ 0.6048 [47]
	GME	≈ 0.479 [46]	≈ 0.6440	≈ 0.5684	≈ 0.7218	≈ 0.6757	$\frac{3}{4} = 0.75$ [48]	≈ 0.7158 [48]

TABLE III: **Critical robustness to white noise w^* for different scenarios.** We provide a comparison between the critical robustness to white noise of the GHZ and W state, in the 4 different scenarios: All 3 parties with trusted devices, *i.e.* using an entanglement witness (EW), 2 or 1 parties with trusted devices, *i.e.* using a steering witness (SW) and no parties with trusted devices *i.e.* nonlocality (DIEW). We give critical values for both detecting entanglement and for detecting genuine multipartite entanglement (\approx refers to numerical results).

bipartition, for which there are a number of different cases, given the asymmetry of the scenario, and finish with the question of detecting genuine multipartite entanglement.

Case 1. Multipartite entanglement

Let us then start by considering a state $\rho^{A:B:C}$ that is fully separable *i.e.*

$$\rho^{A:B:C} = \sum_{\lambda} p_{\lambda} \rho_{\lambda}^A \otimes \rho_{\lambda}^B \otimes \rho_{\lambda}^C, \quad (23)$$

where p_{λ} defines a probability distribution.

Case 1A. Multipartite entanglement with one untrusted party

We treat first the case where a single party, taken to be A, performs a set of untrusted measurements $\{M_{a|x}\}_{a,x}$ on her share of the state, providing the parties B and C with the assemblage

$$\begin{aligned} \sigma_{a|x}^{BC} &= \text{tr}_A(M_{a|x} \otimes \mathbb{1}_B \otimes \mathbb{1}_C \rho^{A:B:C}) \\ &= \sum_{\lambda} p(a|x, \lambda) \rho_{\lambda}^B \otimes \rho_{\lambda}^C. \end{aligned} \quad (24)$$

where $p(a|x, \lambda) = p_{\lambda} \text{tr}(M_{a|x} \rho_{\lambda}^A)$. Notice first that the dependence of Bob and Charlie's assemblage on a and x comes only from the common pre-shared variable λ . This is a typical instance of an unsteerable assemblage, or, in other words, this is a local hidden state (LHS) model for the assemblage $\sigma_{a|x}^{BC}$ [49]. Notice further that it is composed only by separable (unnormalised) states for B and C. Thus, in this case, testing for the presence of multipartite entanglement reduces to testing if the assemblage $\sigma_{a|x}^{BC}$ is steerable and separable at the same

time. This type of assemblages forms a set $\Sigma_{BC}^{A:B:C}$, given by

$$\Sigma_{BC}^{A:B:C} = \left\{ \sigma_{a|x}^{BC} \middle| \sigma_{a|x}^{BC} = \sum_{\mu} D(a|x, \mu) \rho_{\mu}^{BC}, \rho_{\mu}^{BC} \in \text{SEP} \right\} \quad (25)$$

where we have used the fact that any probability distribution $p(a|x, \lambda)$ can be written as a convex combination of deterministic ones $D(a|x, \mu)$, *i.e.* $p_{\lambda}(a|x) = \sum_{\mu} q(\mu|\lambda) D(a|x, \mu)$, and denote the set of (unnormalised) separable quantum states by SEP.

Case 1B. Multipartite entanglement with two untrusted parties

Now we consider that two of the parties, A and B, have untrusted measuring devices. In this case they prepare an assemblage for Charlie, which is given by

$$\begin{aligned} \sigma_{ab|xy}^C &= \text{tr}_{AB}(M_{a|x} \otimes M_{b|y} \otimes \mathbb{1}_C \rho^{A:B:C}) \\ &= \sum_{\lambda} p_{\lambda}(ab|xy) \rho_{\lambda}^C. \end{aligned} \quad (26)$$

Once again, since the only dependence of the assemblage on a, b, x and y is through λ this assemblage is also unsteerable. Moreover, because the set of probability distributions (also called a behaviour) $p_{\lambda}(ab|xy)$ arises from local measurements on a separable state it must be local, *i.e.* it can be written as $p_{\lambda}(ab|xy) = \sum_{\mu\nu} q(\mu\nu|\lambda) D(a|x, \mu) D(b|y, \nu)$ [50]. Therefore, the relevant set of assemblages $\Sigma_C^{A:B:C}$ is now given by

$$\Sigma_C^{A:B:C} = \left\{ \sigma_{ab|xy}^C \middle| \sigma_{ab|xy}^C = \sum_{\mu\nu} D(a|x, \mu) D(b|y, \nu) \rho_{\mu\nu}^C, \rho_{\mu\nu}^C \geq 0 \right\}. \quad (27)$$

Case 2. Entanglement in a bipartition

Let us now consider the case where the state ρ^{ABC} is separable with respect to a single given bipartition. Choosing this partition to be A : BC we now consider states of the form

$$\rho^{A:BC} = \sum_{\lambda} p_{\lambda} \rho_{\lambda}^A \otimes \rho_{\lambda}^{BC}. \quad (28)$$

Crucially, given the asymmetry of picking a bipartition as well as the asymmetry of picking the trusted party (or parties), we will see below that we have two inequivalent situations to consider, for both the cases of one or of two untrusted parties.

Case 2A. Entanglement in a bipartition with one untrusted party

When only one of the parties performs uncharacterised measurements the asymmetry of (28) leads to two different situations: (i) when the lone party A has the untrusted devices and (ii) when B (or equivalently C) does. In the first case Bob

and Charlie's assemblage is given by

$$\begin{aligned}\sigma_{a|x}^{\text{BC}} &= \text{tr}_A(M_{a|x} \otimes \mathbb{1}_B \otimes \mathbb{1}_C \rho^{\text{A:BC}}) \\ &= \sum_{\lambda} p(a|x, \lambda) \rho_{\lambda}^{\text{BC}},\end{aligned}\quad (29)$$

Once again the dependence of Bob and Charlie's assemblage on a and x comes only from the common variable λ , and so this assemblage is unsteerable. In comparison to previously, the states distributed to Bob and Charlie are now arbitrary entangled states, and hence there is no additional structure that the decomposition imposes. The set $\Sigma_{\text{BC}}^{\text{A:BC}}$ defined by assemblages of the form (29) is therefore given by

$$\Sigma_{\text{BC}}^{\text{A:BC}} = \left\{ \sigma_{a|x}^{\text{BC}} \left| \sigma_{a|x}^{\text{BC}} = \sum_{\mu} D(a|x, \mu) \rho_{\mu}^{\text{BC}}, \rho_{\mu}^{\text{BC}} \geq 0 \right. \right\}. \quad (30)$$

In the second case, where Bob is the one not trusting his measurements, Alice and Charlie are left with the following assemblage:

$$\begin{aligned}\sigma_{b|y}^{\text{AC}} &= \text{tr}_B(\mathbb{1}_A \otimes M_{b|y} \otimes \mathbb{1}_C \rho^{\text{A:BC}}) \\ &= \sum_{\lambda} p_{\lambda} \rho_{\lambda}^{\text{A}} \otimes \sigma_{b|y, \lambda}^{\text{C}},\end{aligned}\quad (31)$$

which is a fundamentally different situation. This assemblage now has two main features: (i) the only dependence on the variables b and y are due to Charlie's states. In other words, $\sigma_{b|y}^{\text{AC}}$ is unsteerable from Bob to Alice but not necessarily from Bob to Charlie (note however that the no-signalling condition still holds from Bob to Charlie). This implies that if we trace out system C (or apply any quantum-to-classical map to it) the resulting assemblage for Alice alone will be unsteerable; (ii) it is composed by separable (unnormalised) states. The relevant set, $\Sigma_{\text{AC}}^{\text{A:BC}}$, is now given by

$$\begin{aligned}\Sigma_{\text{AC}}^{\text{A:BC}} &= \left\{ \sigma_{b|y}^{\text{AC}} \left| \text{tr}_C \sigma_{b|y}^{\text{AC}} = \sum_{\mu} D(b|y, \mu) \rho_{\mu}^{\text{A}}, \right. \right. \\ &\quad \left. \rho_{\mu}^{\text{A}} \geq 0, \sigma_{b|y}^{\text{AC}} \in \text{SEP}, \sum_b \sigma_{b|y}^{\text{AC}} = \sum_b \sigma_{b|y'}^{\text{AC}} \right\}\end{aligned}\quad (32)$$

Case 2B. Entanglement in a bipartition with two untrusted parties

Again the asymmetry of the decomposition (28) leads to two different situations: In one the untrusted measurements are at A and B (or similarly A and C), whilst in the other they are at B and C. In the first case the assemblage obtained is given by

$$\begin{aligned}\sigma_{ab|xy}^{\text{C}} &= \text{tr}_{\text{AB}}(M_{a|x} \otimes M_{b|y} \otimes \mathbb{1}_C \rho^{\text{A:BC}}) \\ &= \sum_{\lambda} p(a|x, \lambda) \sigma_{b|y, \lambda}^{\text{C}}.\end{aligned}\quad (33)$$

This assemblage has only one main feature, that it may contain only steering from Bob to Charlie, and not from Alice to

Charlie. It then defines the set $\Sigma_{\text{C}}^{\text{A:BC}}$ as

$$\begin{aligned}\Sigma_{\text{C}}^{\text{A:BC}} &= \left\{ \sigma_{ab|xy}^{\text{C}} \left| \sigma_{ab|xy}^{\text{C}} = \sum_{\mu} D(a|x, \mu) \sigma_{b|y, \mu}^{\text{C}}, \right. \right. \\ &\quad \left. \sigma_{b|y, \mu}^{\text{C}} \geq 0, \sum_b \sigma_{b|y, \mu}^{\text{C}} = \sum_b \sigma_{b|y', \mu}^{\text{C}} \right\}\end{aligned}\quad (34)$$

In the second case the resulting assemblage is given by

$$\begin{aligned}\sigma_{bc|yz}^{\text{A}} &= \text{tr}_{\text{BC}}(\mathbb{1}_A \otimes M_{b|y} \otimes M_{c|z} \rho^{\text{A:BC}}) \\ &= \sum_{\lambda} p(bc|yz, \lambda) \rho_{\lambda}^{\text{A}}.\end{aligned}\quad (35)$$

Here, there are two main features: (i) this assemblage is unsteerable; (ii) The behaviour $p(bc|yz, \lambda)$ arises from local measurements on a possibly entangled state $\rho_{\lambda}^{\text{BC}}$, it may contain nonlocal *quantum* correlations [50]. The final set we define is therefore $\Sigma_{\text{A}}^{\text{A:BC}}$, given by

$$\begin{aligned}\Sigma_{\text{A}}^{\text{A:BC}} &= \left\{ \sigma_{bc|yz}^{\text{A}} \left| \sigma_{bc|yz}^{\text{A}} = \sum_{\lambda} p(bc|yz, \lambda) \rho_{\lambda}^{\text{A}}, \right. \right. \\ &\quad \left. \rho_{\lambda}^{\text{A}} \geq 0, p(bc|yz, \lambda) \in \mathcal{Q} \right\}\end{aligned}\quad (36)$$

where we have denoted by \mathcal{Q} the set of probability distributions which can arise from local measurements on quantum states.

Case 3. Genuine multipartite entanglement

Let us now turn to the question of genuine multipartite entanglement (GME) detection. Genuine tripartite entangled states are the ones that can not be written as

$$\begin{aligned}\rho^{\text{bisep}} &= \sum_{\lambda} p_{\lambda}^{\text{A:BC}} \rho_{\lambda}^{\text{A}} \otimes \rho_{\lambda}^{\text{BC}} + \sum_{\lambda} p_{\lambda}^{\text{B:AC}} \rho_{\lambda}^{\text{B}} \otimes \rho_{\lambda}^{\text{AC}} \\ &\quad + \sum_{\lambda} p_{\lambda}^{\text{AB:C}} \rho_{\lambda}^{\text{AB}} \otimes \rho_{\lambda}^{\text{C}},\end{aligned}\quad (37)$$

where $p_{\lambda}^{\text{A:BC}}$, $p_{\lambda}^{\text{B:AC}}$ and $p_{\lambda}^{\text{AB:C}}$ are probability distributions. Our goal once again is to determine what constraints the form (37) imposes on the obtained assemblages, which will now follow straightforwardly given the analysis made before.

Case 3A. Genuine multipartite entanglement with one untrusted party

When Alice is the one holding the untrusted devices, Bob and Charlie's assemblage is given by

$$\begin{aligned}
\sigma_{a|x}^{\text{BC}} &= \text{tr}(M_{a|x} \otimes \mathbb{1}_B \otimes \mathbb{1}_C \rho^{\text{bisep}}) \\
&= \underbrace{\sum_{\lambda} p_{\lambda}^{\text{A:BC}} p(a|x, \lambda) \rho_{\lambda}^{\text{BC}}}_{\Gamma_{a|x}^{\text{A:BC}} \in \Sigma_{\text{BC}}^{\text{A:BC}}} + \underbrace{\sum_{\lambda} p_{\lambda}^{\text{B:AC}} \rho_{\lambda}^{\text{B}} \otimes \sigma_{a|x, \lambda}^{\text{C}}}_{\Gamma_{a|x}^{\text{B:AC}} \in \Sigma_{\text{BC}}^{\text{B:AC}}} + \underbrace{\sum_{\lambda} p_{\lambda}^{\text{AB:C}} \sigma_{a|x, \lambda}^{\text{B}} \otimes \rho_{\lambda}^{\text{C}}}_{\Gamma_{a|x}^{\text{C:AB}} \in \Sigma_{\text{BC}}^{\text{C:AB}}}.
\end{aligned} \tag{38}$$

The terms $\Gamma_{a|x}^{\text{A:BC}}$ and $\Gamma_{a|x}^{\text{B:AC}}$ can be seen as assemblages having the same structure as the assemblages (29) and (31) respectively, while the assemblage $\Gamma_{a|x}^{\text{C:AB}}$ is identical to $\Gamma_{a|x}^{\text{B:AC}}$, except that the role of Bob and Charlie is interchanged.

Case 3B. Genuine multipartite entanglement with two untrusted parties

Consider now that Alice and Bob perform untrusted measurements, leading to:

$$\begin{aligned}
\sigma_{ab|xy}^{\text{C}} &= \text{tr}_{\text{AB}}(M_{a|x} \otimes M_{b|y} \otimes \mathbb{1}_C \rho^{\text{bisep}}) \\
&= \underbrace{\sum_{\lambda} p_{\lambda}^{\text{A:BC}} p(a|x, \lambda) \sigma_{b|y, \lambda}^{\text{C}}}_{\Pi_{ab|xy}^{\text{A:BC}} \in \Sigma_{\text{C}}^{\text{A:BC}}} + \underbrace{\sum_{\lambda} p_{\lambda}^{\text{B:AC}} p(b|y, \lambda) \sigma_{a|x, \lambda}^{\text{C}}}_{\Pi_{ab|xy}^{\text{B:AC}} \in \Sigma_{\text{C}}^{\text{B:AC}}} + \underbrace{\sum_{\lambda} p_{\lambda}^{\text{AB:C}} p(ab|xy, \lambda) \rho_{\lambda}^{\text{C}}}_{\Pi_{ab|xy}^{\text{C:AB}} \in \Sigma_{\text{C}}^{\text{C:AB}}}.
\end{aligned} \tag{39}$$

Again, the assemblages $\Pi_{ab|xy}^{\text{A:BC}}$ and $\Pi_{ab|xy}^{\text{B:AC}}$ are seen to have the same structure as (33), while the assemblage $\Pi_{ab|xy}^{\text{C:AB}}$ has the same structure as (35).

Supplementary note 2

SDP tests and semi-device-independent entanglement witnesses

We have previously determined the constraints that each kind of entanglement imposes, and defined the corresponding sets of assemblages these constraints define. We now turn to the following practical question: given that we have observed a specific assemblage, can we test for a certain type of entanglement by checking whether or not the assemblage belongs to one of the previously defined sets?

Crucially, it turns out that all of the sets defined above are either specified solely in terms of positive semi-definite (PSD) constraints and linear matrix inequalities (LMIs), or can be approximated from the outside by a set with such a specification. Testing for membership inside such a set is an optimisation problem known as a semi-definite program (SDP), for which efficient numerical methods exist for the case of small systems, allowing for an answer to this question [51]. More-

over, due to the theory of duality, the dual SDP provides us with a semi-device-independent witness that allow us to certify the presence of the different types of entanglement solely from the knowledge of the assemblage. This is similar to the ideas of entanglement witnesses and Bell inequalities in the standard and fully device-independent scenarios respectively.

1. Deriving the SDP tests

In those cases where the the sets defined above are not specified solely in terms of PSD constraints and LMIs our strategy is to show that there exist suitable relaxations which are, that is to define bigger sets which are specified solely in terms of such constraints.

Working through in the order that they appeared, we shall consider each set in turn. The first set is $\Sigma_{\text{BC}}^{\text{A:BC}}$, given in equation (25). It is the final constraint, $\rho_{\mu}^{\text{BC}} \in \text{SEP}$, that does not have the desired form, as the set of (unnormalised) separable states has in general a complicated structure. The one case where the set in fact has a simple characterisation is if the dimensions satisfy $d_B d_C \leq 6$, in which case the set of separable states is exactly the set of states positive under partial transposition (PPT) [52]. In this simple case we can

rewrite $\rho_\mu^{\text{BC}} \in \text{SEP}$ as $(\rho_\mu^{\text{BC}})^{\text{T}_B} \geq 0$, where T_B denotes the partial transposition with respect to system B. Since this operation is a linear map (on the state), this is now a PSD constraint, and the set is in fact in the desired form.

In all other dimensions, we can use the relaxation of the separable states to those that have a k -symmetric PPT extension [53]. That is, we define the set $\text{SYM}_{\text{BC}}^{(k)}$

$$\text{SYM}_{\text{BC}}^{(k)} = \left\{ \rho^{\text{BC}} \left| \begin{aligned} \rho^{\text{BC}} &= \text{tr}_{\text{B}_2 \dots \text{B}_k} \rho^{\text{B}_1 \dots \text{B}_k \text{C}}, \\ S_{ij} \rho^{\text{B}_1 \dots \text{B}_k \text{C}} S_{ij}^\dagger &= \rho^{\text{B}_1 \dots \text{B}_k \text{C}} \quad \forall i \neq j, \\ (\rho^{\text{B}_1 \dots \text{B}_k \text{C}})^{\text{T}_C} &\geq 0, \rho^{\text{B}_1 \dots \text{B}_k \text{C}} \geq 0 \end{aligned} \right. \right\} \quad (40)$$

where S_{ij} is the swap operator between B_i and B_j . This demands that ρ^{BC} can be extended to a state with k Bobs, which is symmetric under interchange and PPT, such that the reduced state of a single Bob and Charlie is the original state. Such sets are all specified in terms of PSD constraints and LMIs, and converge to the set of separable states as $k \rightarrow \infty$ [53, 54]. For the case $k = 1$ it also reduces to the set of PPT state. We thus define the sequence of relaxations

$$\Sigma_{\text{BC}}^{\text{A:B:C}(k)} = \left\{ \sigma_{a|x}^{\text{BC}} \left| \begin{aligned} \sigma_{a|x}^{\text{BC}} &= \sum_\mu D(a|x, \mu) \rho_\mu^{\text{BC}}, \\ \rho_\mu^{\text{BC}} &\in \text{SYM}_{\text{BC}}^{(k)} \end{aligned} \right. \right\}, \quad (41)$$

which now have the desired structure for each k .

Moving on, the set $\Sigma_{\text{C}}^{\text{A:B:C}}$ given in (27) already has the desired structure. This is also true for the set $\Sigma_{\text{BC}}^{\text{A:BC}}$ defined in (30). The set $\Sigma_{\text{AC}}^{\text{A:BC}}$ (32) contains the requirement that $\sigma_{b|y}^{\text{AC}} \in \text{SEP}$, which is dealt with in exactly the same way as above. Thus we define the relaxed set

$$\Sigma_{\text{AC}}^{\text{A:BC}(k)} = \left\{ \sigma_{b|y}^{\text{AC}} \left| \begin{aligned} \text{tr}_C \sigma_{b|y}^{\text{AC}} &= \sum_\mu D(b|y, \mu) \rho_\mu^{\text{A}}, \\ \rho_\mu^{\text{A}} &\geq 0, \sigma_{b|y}^{\text{AC}} \in \text{SYM}_{\text{AC}}^{(k)}, \sum_b \sigma_{b|y}^{\text{AC}} = \sum_b \sigma_{b|y'}^{\text{AC}} \end{aligned} \right. \right\} \quad (42)$$

The set $\Sigma_{\text{C}}^{\text{A:BC}}$ given in (34) has the desired structure.

Finally, the set $\Sigma_{\text{C}}^{\text{C:AB}}$ (which has the same structure as (36)) is less straightforward because of the constraint $p(ab|xy, \lambda) \in \mathcal{Q}$, i.e. that the behaviours $p(ab|xy, \lambda)$ should have a quantum realisation. As in the nonlocality scenario of deciding if a behaviour has a quantum realisation, the exact answer to this problem is in general intractable. However, we can use the idea introduced in [55] (see also [56]) to obtain a semi-definite relaxation. The basic idea is to apply the method of the NPA hierarchy [57] only to the untrusted devices, whilst leaving Charlie quantum, using also the fact that the state is separable on the $\text{AB} : \text{C}$ partition. We thus relax to $\Pi_{ab|xy}^{\text{C:AB}} \in \mathcal{Q}_{\text{C}}^{(k)}$, where $\mathcal{Q}_{\text{C}}^{(k)}$ is defined by

$$\mathcal{Q}_{\text{C}}^{(k)} = \left\{ \sigma_{ab|xy}^{\text{C}} \left| \begin{aligned} \Gamma_{\text{C}}^{(k)} &\geq 0, \left(\Gamma_{\text{C}}^{(k)} \right)^{\text{T}_C} \geq 0 \\ \text{tr} \left(G_j \Gamma_{\text{C}}^{(k)} \right) &= \text{tr} \left(h_j \sigma_{ab|xy}^{\text{C}} \right) \forall j \end{aligned} \right. \right\} \quad (43)$$

for some sets of operators $\{G_j^{(k)}\}$ and $\{h_j^{(k)}\}$, which encode the constraints that arise in the original NPA hierarchy [57], coming from (i) orthogonality of measurement outcomes, and (ii) commutivity of Alices and Bob measurements. Also, we can apply the idea from [55] and impose that the matrices $\Gamma_{\text{C}}^{(k)}$ are positive under partial transposition of Charlie (the trusted party), as a relaxation of the separability criteria across the bipartition. The main difference with the NPA approach is that whereas previously the elements of the matrix $\Gamma_{\text{C}}^{(k)}$ were complex numbers with certain ones equal to the nonlocal behaviour, now one should think of the elements as matrices (of the dimension of Charlie), with certain ones equal to members of the assemblage.

Last, in order to be able to impose semidefinite constraints to the set $\Sigma_{\text{C}}^{\text{C:AB}}$ we need to constrain the number of terms in the summation in λ . We do this by noticing that any quantum behaviour can be written as a convex combination of extremal non-signalling behaviours $D^{\text{NS}}(bc|yz, \nu)$ [50].

Given the above, set $\Sigma_{\text{A}}^{\text{C:AB}}$ is relaxed to

$$\Sigma_{\text{C}}^{\text{C:AB}(k)} = \left\{ \sigma_{ab|xy}^{\text{C}} \left| \begin{aligned} \sigma_{ab|xy}^{\text{C}} &= \sum_\nu D^{\text{NS}}(ab|xy, \nu) \sigma_\nu^{\text{C}}, \\ \sigma_{ab|xy}^{\text{C}} &\in \mathcal{Q}_{\text{C}}^{(k)} \end{aligned} \right. \right\}. \quad (44)$$

Having found appropriate relaxations of all of the sets which we wish to consider, we can now straightforwardly write down an approximate optimisation problem in the form of an SDP that needs to be solved to check for the desired type of entanglement in each given scenario. Let us describe explicitly the approximate test that checks for the existence of a decomposition of the form (39), i.e. that checks for genuine multipartite entanglement with two untrusted parties. We provide all the other SDP tests for the other decompositions described above in Supplementary Table II.

In (39) we see that we have to find 3 assemblages, each contained in a different set, with each set either in a form directly usable, or for which we just gave an outer approximation above. Thus, by introducing the *maximally mixed assemblage* $\text{id}_{ab|xy}^{\text{C}} = \frac{1}{m_{\text{A}} m_{\text{B}}} \mathbb{1}_{\text{C}} / d_{\text{C}}$ we arrive at the following SDP test for genuine multipartite entanglement with 2 untrusted parties

$$\begin{aligned} \max \quad & p \\ \text{s.t.} \quad & \Pi_{ab|xy}^{\text{A:BC}} + \Pi_{ab|xy}^{\text{B:AC}} + \Pi_{ab|xy}^{\text{C:AB}} = \sigma_{ab|xy}^{\text{obs}} - p \text{id}_{ab|xy}^{\text{C}} \\ & \Pi_{ab|xy}^{\text{A:BC}} \in \Sigma_{\text{C}}^{\text{A:BC}}, \Pi_{ab|xy}^{\text{B:AC}} \in \Sigma_{\text{C}}^{\text{B:AC}}, \\ & \Pi_{ab|xy}^{\text{C:AB}} \in \Sigma_{\text{C}}^{\text{C:AB}(k)} \end{aligned} \quad (45)$$

where $\sigma_{ab|xy}^{\text{obs}}$ is the observed assemblage of Charlie. Since $\text{id}_{ab|xy}^{\text{C}}$ is clearly contained in all 3 sets, being producible from the maximally mixed state, a sufficiently large negative p will always be a solution, hence the SDP is strictly feasible. A strictly negative optimal solution $p^* < 0$ certifies that $\sigma_{ab|xy}^{\text{obs}}$ being measured does not have the desired decomposition, i.e. that the state is genuinely multipartite entangled. On the other hand an optimal value $p^* = 0$ indicates that a decomposition can be found. Note however that in this case, given the relaxation of the problem, one is not able to conclude anything

regarding the separability of the state. One can take the parameter k larger to obtain a better approximation to the original problem.

2. Semi device-independent entanglement witnesses

The dual of the SDP (45) is also readily written down [51], and is given by

$$\begin{aligned}
\min \quad & \text{tr} \sum_{abxy} F_{ab|xy} \sigma_{ab|xy}^{\text{obs}} \\
\text{s.t.} \quad & \text{tr} \sum_{abxy} F_{ab|xy} \sigma_{ab|xy}^C \geq 0 \\
& \forall \sigma_{ab|xy}^C \in \Sigma_C^{A:BC} \cup \Sigma_C^{B:AC} \cup \Sigma_C^{C:AB(k)} \quad (46) \\
& \text{tr} \sum_{abxy} F_{ab|xy} \text{id}_{ab|xy}^C = 1
\end{aligned}$$

which is seen to constitute a witness for genuine multipartite entanglement. That is, the dual provides a set of operators $\{F_{ab|xy}\}_{abxy}$ such that the linear functional $\beta = \sum_{abxy} F_{ab|xy} \sigma_{ab|xy}$ is greater than zero for all assemblages which arise from measurements on a bi-separable state. An observed value $\beta^{\text{obs}} < 0$ thus provides a witness which certifies the genuine multipartite entanglement of the state in a semi-device-independent manner. The final condition, $\text{tr} \sum_{abxy} F_{ab|xy} \text{id}_{ab|xy}^C = 1$ is a convention, which simply defines an overall scale for the witness.

More generally, the dual of each SDP in Supplementary Table II provides witness operators $\{F_{a|x}\}_{ax}$, for the case of Alice untrusted, or $\{F_{ab|xy}\}_{abxy}$, for the case of Alice and Bob untrusted (or a permutation of the parties) which constitute a semi-device-independent entanglement witnesses of the form

$$\begin{aligned}
& \text{tr} \sum_{ax} F_{a|x} \sigma_{a|x} \geq 0 \quad \forall \sigma_{a|x} \in \Sigma \\
& \text{tr} \sum_{abxy} F_{ab|xy} \sigma_{ab|xy} \geq 0 \quad \forall \sigma_{ab|xy} \in \Sigma' \quad (47)
\end{aligned}$$

with corresponding violations $\beta^{\text{obs}} = \text{tr} \sum_{ax} F_{a|x} \sigma_{a|x}^{\text{obs}} < 0$ or $\beta^{\text{obs}} = \text{tr} \sum_{abxy} F_{ab|xy} \sigma_{ab|xy}^{\text{obs}} < 0$ respectively, where Σ and Σ' are sets, or union of sets (depending upon the type of entanglement one is checking for), as defined above.

Finally, we note that it is possible to put these witnesses into two more friendly forms in the case of binary measurement outcomes, so-called *observable* and *coefficient* forms. Starting with the observable form, we use the definition of the observed assemblage, and introduce the observables $A_x =$

$M_{0|x} - M_{1|x}$ to arrive at

$$\begin{aligned}
& \text{tr} \sum_{ax} F_{a|x} \sigma_{a|x}^{\text{obs}} = \text{tr} \sum_{ax} M_{a|x} \otimes F_{a|x} \rho \\
& = \frac{1}{2} \text{tr} \sum_{ax} (\mathbb{1}_A + (-1)^a A_x) \otimes F_{a|x} \rho \\
& = \text{tr} (\mathbb{1}_A \otimes \frac{1}{2} \sum_{ax} F_{a|x} + \sum_x A_x \otimes \frac{1}{2} \sum_a (-1)^a F_{a|x}) \rho \\
& = \text{tr} (\mathbb{1}_A \otimes J_\emptyset + \sum_x A_x \otimes J_x) \rho \quad (48)
\end{aligned}$$

for the case of one untrusted party, where we have defined the observables $J_\emptyset = \frac{1}{2} \sum_{ax} F_{a|x}$ and $J_x = \frac{1}{2} \sum_a (-1)^a F_{ab|xy}$ for Bob and Charlie. For the coefficient form we further expand these matrices in the (complete) basis of Pauli operators, namely,

$$J_\emptyset = \sum_{yz} f_{0yz} \sigma^y \otimes \sigma^z, \quad J_x = \sum_{yz} f_{xyz} \sigma^y \otimes \sigma^z \quad (49)$$

where $\sigma^0 = \mathbb{1}$, $\sigma^1 = X$, $\sigma^2 = Y$ and $\sigma^3 = Z$ and denoting $A_0 = \mathbb{1}$ then we arrive at the compact form

$$\text{tr} \sum_{ax} F_{a|x} \sigma_{a|x}^{\text{obs}} = \text{tr} \left(\sum_{xyz} (f_{xyz} A_x \otimes \sigma^y \otimes \sigma^z) \rho \right) \quad (50)$$

For the case of two untrusted parties, an analogous but longer calculation gives for the observable form

$$\begin{aligned}
& \text{tr} \sum_{abxy} F_{ab|xy} \sigma_{ab|xy}^{\text{obs}} \\
& = \text{tr} (\mathbb{1}_A \otimes \mathbb{1}_B \otimes K_\emptyset + \sum_x A_x \otimes \mathbb{1}_B \otimes K_x \\
& + \sum_y \mathbb{1}_A \otimes B_y \otimes K'_y + \sum_{xy} A_x \otimes B_y \otimes K_{xy}) \rho \quad (51)
\end{aligned}$$

where we have introduced the observables B_y for Bob, as well as the observables $K_\emptyset = \frac{1}{4} \sum_{abxy} F_{ab|xy}$, $K_x = \frac{1}{4} \sum_{aby} (-1)^a F_{ab|xy}$, $K'_y = \frac{1}{4} \sum_{abx} (-1)^b F_{ab|xy}$ and $K_{xy} = \frac{1}{4} \sum_{ab} (-1)^{a+b} F_{ab|xy}$ for the trusted party Charlie, that need to be measured in the corresponding configurations, given above. For the coefficient form, again by expanding these matrices in the complete basis of Pauli matrices,

$$\begin{aligned}
K_\emptyset &= \sum_z f_{00z} \sigma^z, & K_x &= \sum_z f_{x0z} \sigma^z \\
K'_y &= \sum_z f_{0yz} \sigma^z, & K_{xy} &= \sum_z f_{xyz} \sigma^z \quad (52)
\end{aligned}$$

and by denoting $B_0 = \mathbb{1}$, we obtain the analogous compact form as previously,

$$\text{tr} \sum_{abxy} F_{ab|xy} \sigma_{ab|xy}^{\text{obs}} = \text{tr} \left(\sum_{xyz} (f_{xyz} A_x \otimes B_y \otimes \sigma^z) \rho \right) \quad (53)$$

Supplementary note 3

Generalisation to more parties

We have presented our main results in the tripartite case. Notice however that the same procedure can readily be followed to derive SDPs to test the presence of different kinds of entanglement for general N -partite systems.

First of all one specifies the scenarios by fixing (i) a particular type of entanglement and (ii) the pattern of trusted and untrusted parties. The entanglement can be chosen arbitrarily, for example one may ask that the state is not fully separable, be separable across a given number of fixed bipartitions, or be a convex combination of states separable over a given number of partitions (but not necessarily fixed). The pattern may also be chosen arbitrarily, ranging from all but one party trusted, to all but one untrusted.

Given the specification, one then enumerates the list of properties which the corresponding assemblages have. These properties will fall into two classes - those which impose constraints which are directly applicable, *i.e.* are in the form of PSD constraints and LMIs, and those which are not. As in the tripartite case, the objective is then to relax the non-directly applicable constraints to find an approximate SDP test.

The main difficulty in our approach is that as the number of parties increases, and the local dimension of the Hilbert space, we expect that the difficulty of the problem will grow to the point where current numerical techniques are unable to solve efficiently the tests. For example, one class of constraints that will arise is that multipartite assemblages will need to have quantum realisations. In principle such a constraint can still be imposed by applying the NPA hierarchy [57] to the untrusted devices, however in the multipartite setting this soon becomes intractable. Alternatively, one may have constraints that a multipartite quantum state is separable. One can again relax this using the generalisation of the k -shareability condition [54].

In summary, the approach presented here is most suitable to scenarios involving relatively small numbers of parties, where it provides powerful tests for multipartite entanglement (and explicitly provides witnesses in each case). This is however expected as this is also the case in standard entanglement detection techniques [58] (due to the increase of the Hilbert space dimension) and in the fully device-independent approach [50] (due to the number of the space of local probability distributions).

Supplementary note 4

Examples: GHZ and W states

In order to demonstrate the usefulness of our previous characterisation we apply the above SDP to two exemplary genuine multipartite states, namely the GHZ and W states. More specifically we are interested in how much white noise can be added to these states until our method fails to detect ei-

ther entanglement or GME, *i.e.* we want find the minimum w , denoted by w^* , allowing us to detect either entanglement or GME in the states

$$\begin{aligned}\rho_{\text{GHZ}} &= w|\text{GHZ}\rangle\langle\text{GHZ}| + (1-w)\mathbb{1}/8; \\ \rho_W &= w|W\rangle\langle W| + (1-w)\mathbb{1}/8,\end{aligned}\quad (54)$$

where $|\text{GHZ}\rangle = (|000\rangle + |111\rangle)/\sqrt{2}$ and $|W\rangle = (|001\rangle + |010\rangle + |100\rangle)/\sqrt{3}$. Supplementary Table III gives a summary of the results, in terms of the numbers provided by our methods and a comparison to what was known regarding entanglement witnesses and Bell inequalities. All results were obtained using CVX [51] for MATLAB to solve the SDP, and the optimisation toolbox to numerically search for the best choices of measurements for Alice (and Bob). Since such a search over measurements choices provides no guarantee that the global optimum is obtained, all results constitute upper bounds. However, all of our numerical evidence suggests that the values obtained cannot be improved.

As we can see the values of w^* lies in between the bound for entanglement, where the largest number of assumptions are made, and the bound from nonlocality, where no assumptions are made. Furthermore, as one would expect, stronger bounds are possible with 2 parties trust their devices compared to the case of only 1.

We end by presenting the steering witnesses we obtain in the above for the GHZ and W states that certify genuine tripartite entanglement in a semi-device-independent fashion.

Starting with the GHZ state and the case of two untrusted parties (and three measurements), the optimal witness is

$$\begin{aligned}1 - \alpha\langle A_2 B_2 \rangle - \alpha\langle A_2 Z \rangle - \alpha\langle B_2 Z \rangle - \beta\langle A_0 B_0 X \rangle \\ + \beta\langle A_0 B_1 Y \rangle + \beta\langle A_1 B_0 Y \rangle + \beta\langle A_1 B_1 X \rangle \geq 0\end{aligned}\quad (55)$$

where $\alpha = 0.1831$ and $\beta = 0.2582$, and the pure GHZ state achieves a violation $-0.5821 \not\geq 0$. For the case of the GHZ state and only a single untrusted party, the witness is

$$\begin{aligned}1 + 0.1547\langle Z_B Z_C \rangle - \frac{1}{3}(\langle A_2 Z_B \rangle + \langle A_2 Z_C \rangle + \langle A_0 X_B X_C \rangle \\ - \langle A_0 Y_B Y_C \rangle - \langle A_1 X_B Y_C \rangle - \langle A_1 Y_B X_C \rangle) \geq 0\end{aligned}\quad (56)$$

with the pure GHZ state now achieving a violation of $-0.8453 \not\geq 0$. Interestingly, we note first that the structure of both witnesses is the same, the only difference being in the coefficients. Furthermore the only terms which appear are those which arise from the stabiliser relations of the GHZ state.

Moving on to the W state, for two untrusted parties the optimal witness is

$$\begin{aligned}1 + 0.2517(\langle A_2 \rangle + \langle B_2 \rangle) + 0.3520\langle Z \rangle - 0.1112(\langle A_0 X \rangle \\ + \langle A_1 Y \rangle + \langle B_0 X \rangle + \langle B_1 Y \rangle) + 0.1296(\langle A_2 Z \rangle + \langle B_2 Z \rangle) \\ - 0.1943(\langle A_0 B_0 \rangle + \langle A_1 B_1 \rangle) + 0.2277\langle A_2 B_2 \rangle \\ - 0.1590(\langle A_0 B_0 Z \rangle + \langle A_1 B_1 Z \rangle) + 0.2228\langle A_2 B_2 Z \rangle \\ - 0.2298(\langle A_0 B_2 X \rangle + \langle A_1 B_2 Y \rangle + \langle A_2 B_0 X \rangle + \langle A_2 B_1 Y \rangle) \geq 0\end{aligned}\quad (57)$$

and the pure W state obtains the violation $-0.4803 \not\geq 0$. For one untrusted party the witness is

$$1 + 0.4405(\langle Z_B \rangle + \langle Z_C \rangle) - 0.0037\langle Z_B Z_C \rangle - 0.1570(\langle X_B X_C \rangle + \langle Y_B Y_C \rangle + \langle A_2 X_B X_C \rangle + \langle A_2 Y_B Y_C \rangle) + 0.2424(\langle A_2 \rangle + \langle A_2 Z_B Z_C \rangle) + 0.1848(\langle A_2 Z_B \rangle + \langle A_2 Z_C \rangle) - 0.2533(\langle A_0 X_B \rangle + \langle A_0 X_C \rangle + \langle A_1 Y_B \rangle + \langle A_1 Y_C \rangle + \langle A_0 X_B Z_C \rangle + \langle A_0 Z_B X_C \rangle + \langle A_1 Y_B Z_C \rangle + \langle A_1 Z_B Y_C \rangle) \geq 0 \quad (58)$$

with the pure W state achieving the violation $-0.7594 \not\geq 0$. Again, we note that structurally the witnesses are the same in the case of one and two untrusted parties.

Supplementary note 5

Experimental inequalities

In this section we give the semi-device independent entanglement witnesses that were used to optimally certify the presence of genuine multipartite entanglement of the GHZ state. Starting with the case of one untrusted party, in coefficient form the inequality is given by

$$\begin{aligned} f_{xy0} &= \begin{pmatrix} 1.0000 & -0.0183 & 0.1079 & 0.0130 \\ 0.1522 & 0.1518 & -0.0734 & 0.0251 \\ -0.2870 & -0.1125 & -0.1229 & 0.0189 \\ -0.0658 & 0.0095 & -0.0151 & -0.2142 \end{pmatrix}, \\ f_{xy1} &= \begin{pmatrix} 0.2096 & 0.0941 & 0.1565 & 0.0077 \\ 0.0633 & 0.3006 & -0.0195 & 0.0132 \\ -0.0388 & -0.0133 & -0.3040 & -0.0033 \\ 0.0614 & 0.0040 & -0.0389 & -0.0387 \end{pmatrix}, \\ f_{xy2} &= \begin{pmatrix} -0.1487 & -0.1841 & 0.0862 & -0.0061 \\ -0.1839 & 0.0323 & 0.2801 & 0.0028 \\ 0.1036 & 0.2920 & -0.0423 & 0.0071 \\ 0.0066 & 0.0683 & 0.0277 & 0.0242 \end{pmatrix}, \\ f_{xy3} &= \begin{pmatrix} 0.0189 & 0.0114 & 0.0363 & -0.2187 \\ -0.0259 & -0.0144 & 0.0255 & -0.0204 \\ -0.0714 & -0.0027 & 0.0099 & 0.0505 \\ -0.0189 & 0.1263 & -0.2037 & 0.0145 \end{pmatrix}, \end{aligned} \quad (59)$$

where x labels the rows and y the columns. For two untrusted parties the inequality is given by

$$\begin{aligned} f_{xy0} &= \begin{pmatrix} 1.0000 & 0.2375 & -0.2613 & 0.0023 \\ 0.0026 & -0.0041 & -0.0055 & 0.0241 \\ -0.0039 & -0.0055 & -0.0114 & 0.0291 \\ -0.0012 & 0.0014 & 0.0032 & -0.1515 \end{pmatrix}, \\ f_{xy1} &= \begin{pmatrix} 0.0041 & -0.0033 & -0.0022 & 0.0275 \\ 0.1673 & 0.2676 & -0.0317 & 0.0044 \\ 0.1710 & -0.0015 & -0.2737 & -0.0072 \\ 0.0009 & 0.0059 & 0.0004 & 0.0001 \end{pmatrix}, \\ f_{xy2} &= \begin{pmatrix} -0.0063 & -0.0091 & 0.0053 & 0.0106 \\ -0.1669 & -0.0004 & 0.2651 & 0.0073 \\ 0.1675 & 0.2569 & -0.0307 & 0.0036 \\ 0.0019 & 0.0161 & 0.0127 & 0.0004 \end{pmatrix}, \\ f_{xy3} &= \begin{pmatrix} -0.0013 & 0.0054 & 0.0011 & -0.1523 \\ 0.0024 & 0.0089 & 0.0053 & 0.0002 \\ 0.0023 & 0.0053 & 0.0047 & 0.0001 \\ -0.1527 & -0.0050 & -0.0085 & -0.0014 \end{pmatrix}. \end{aligned} \quad (60)$$

-
- [1] O. Gühne and G. Tóth, Entanglement detection, *Phys. Rep.* **474**, 1-75 (2009).
[2] D. Rosset, R. Ferretti-Schöbitz, J.-D. Bancal, N. Gisin, and Y.-C. Liang, Imperfect measurement settings: Implications for quantum state tomography and entanglement witnesses, *Phys. Rev. A* **86**, 062325 (2012).
[3] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani and S. Wehner, Bell nonlocality, *Rev. Mod. Phys.* **86**, 419-478 (2014).
[4] J. S. Bell, *Physics* (College. Park. Md), **1**, 195 (1964).
[5] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, V. Scarani, Device-independent security of quantum cryptography against collective attacks, *Phys. Rev. Lett.* **98**, 230501 (2007).
[6] L. Lydersen et al., Hacking commercial quantum cryptography systems by tailored bright illumination, *Nat. Phot.* **4**, 686179 (2010);
[7] I. Gerhardt et al., Full-field implementation of a perfect eavesdropper on a quantum cryptography system, *Nature Comm.* **2**, 349 (2011).
[8] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, V. Scarani, V. Makarov, C. Kurtsiefer, Experimentally faking the violation of Bell's inequalities, *Phys. Rev. Lett.* **107**, 170404 (2011).
[9] E. Schrödinger, *Proc. Camb. Phil. Soc.* **31**, 555-563 (1935).
[10] H.M. Wiseman, S.J. Jones and A.C. Doherty, Steering, Entanglement, Nonlocality, and the EPR Paradox, *Phys. Rev. Lett.* **98**, 140402 (2007);
[11] C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, H. M. Wiseman, One-sided Device-Independent Quantum Key Distribution: Security, feasibility, and the connection with steering,

- Phys. Rev. A **85**, 010301(R) (2012).
- [12] Yun Zhi Law, Le Phuc Thinh, Jean-Daniel Bancal, Valerio Scarani, Quantum randomness extraction for various levels of characterization of the devices, J. Phys. A: Math. Theor. **47**, 424028 (2014).
 - [13] Z. Y. Ou, S. F. Pereira, H. J. Kimble, and K. C. Peng, Realization of the Einstein-Podolsky-Rosen paradox for continuous variables Phys. Rev. Lett. **68**, 3663 (1992).
 - [14] W. P. Bowen, R. Schnabel, P. K. Lam, and T. C. Ralph, Experimental Investigation of Criteria for Continuous Variable Entanglement, Phys. Rev. Lett. **90**, 043601 (2003).
 - [15] D. J. Saunders, S. J. Jones, H. M. Wiseman and G. J. Pryde, Experimental EPR-Steering using Bell-local States, Nat. Phys. **6**, 845-849 (2010).
 - [16] D.-H. Smith *et al.*, Conclusive quantum steering with superconducting transition edge sensors, Nat. Commun. **3**, 625 (2012);
 - [17] A. J. Bennet *et al.*, Arbitrarily loss-tolerant Einstein-Podolsky-Rosen steering allowing a demonstration over 1 km of optical fiber with no detection loophole, Phys. Rev. X **2**, 031003 (2012);
 - [18] V. Händchen *et al.*, Observation of one-way Einstein-Podolsky-Rosen steering, Nat. Phot. **6**, 596179 (2012);
 - [19] B. Wittmann *et al.*, Loophole-free Einstein-Podolsky-Rosen experiment via quantum steering, New J. Phys. **14**, 053030 (2012);
 - [20] G. Svetlichny, Distinguishing three-body from two-body non-separability by a Bell-type inequality, Phys. Rev. D **35**, 3066-3069 (1987);
 - [21] M. Seevinck and G. Svetlichny, Bell-Type Inequalities for Partial Separability in N-Particle Systems and Quantum Mechanical Violations, Phys. Rev. Lett. **89**, 060401 (2002);
 - [22] D. Collins, N. Gisin, S. Popescu, D. Roberts, V. Scarani, Bell-Type Inequalities to Detect True n-Body Nonseparability, Phys. Rev. Lett. **88**, 170405 (2002);
 - [23] J.-D. Bancal, N. Gisin, Y.-C. Liang, and S. Pironio, Device-Independent Witnesses of Genuine Multipartite Entanglement, Phys. Rev. Lett. **106**, 250404 (2011).
 - [24] J. T. Barreiro, J.-D. Bancal, P. Schindler, D. Nigg, M. Hennrich, T. Monz, N. Gisin, and R. Blatt, Demonstration of genuine multipartite entanglement with device-independent witnesses, Nat. Phys. **9**, 559 (2013).
 - [25] M. McKague, Self-Testing Graph States, Lecture Notes in Computer Science **6745**, 104-120 (2014).
 - [26] K. F. Pal, T. Vertesi, M. Navascués, Device-independent tomography of multipartite quantum states, Phys. Rev. A **90**, 042340 (2014).
 - [27] X. Wu, Y. Cai, T. Haur Yang, H. Nguyen Le, J.-D. Bancal, V. Scarani, Robust self testing of the 3-qubit W state, Phys. Rev. A **90**, 042339 (2014).
 - [28] E. G. Cavalcanti, Q. Y. He, M. D. Reid, H. M. Wiseman, Unified criteria for multipartite quantum nonlocality, Phys. Rev. A **84**, 032115 (2011).
 - [29] A. Pappa, A. Chailloux, S. Wehner, E. Diamanti, and I. Kerenidis, Multipartite Entanglement Verification Resistant against Dishonest Parties, Phys. Rev. Lett. **108**, 260502 (2012).
 - [30] Q. Y. He, M. D. Reid, Genuine multipartite Einstein-Podolsky-Rosen steering, Phys Rev Lett. **111**, 250403 (2013).
 - [31] S. Armstrong, M. Wang, R. Yan Teh, Q. Gong, Q. He, J. Janousek, H.-A. Bachor, M. D. Reid, P. K. Lam, Multipartite Einstein-Podolsky-Rosen steering and genuine tripartite entanglement with optical networks, Nature Physics **11**, 167172 (2015).
 - [32] C.-M. Li, K. Chen, Y.-N. Chen, Q. Zhang, Y.-A. Chen and J.-W. Pan, Genuine High-Order Einstein-Podolsky-Rosen Steering. Preprint at <http://arxiv.org/abs/1501.01452> (2015).
 - [33] P. Shadbolt, T. Vertesi, Y.-C. Liang, C. Branciard, N. Brunner, J. L. O'Brien, Guaranteed violation of a Bell inequality without aligned reference frames or calibrated devices, Scientific Reports **2**, 470 (2012).
 - [34] L. Gurvits, Classical complexity and quantum entanglement, J. Comp. Sys. Sci. **69**, 448174 (2004).
 - [35] M. Navascués, S. Pironio, and A. Acín, Bounding the Set of Quantum Correlations, Phys. Rev. Lett. **98**, 10401 (2007);
 - [36] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Distinguishing Separable and Entangled States, Phys. Rev. Lett. **88**, 187904 (2002);
 - [37] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Detecting multipartite entanglement, Phys. Rev. A **71**, 032333 (2005).
 - [38] O. Gühne and M. Seevinck, Separability criteria for genuine multiparticle entanglement, New J. Phys. **12**, 053002 (2010).
 - [39] B. Jungnitsch, T. Moroder, and O. Gühne, Taming multiparticle entanglement, Phys. Rev. Lett. **106**, 190502 (2011).
 - [40] O. Jiménez Farías, G. H. Aguilar, A. Valdés-Hernández, P. H. Souto Ribeiro, L. Davidovich, and S. P. Walborn, Observation of the Emergence of Multipartite Entanglement Between a Bipartite System and its Environment, Phys. Rev. Lett. **109**, 150403 (2012).
 - [41] G. H. Aguilar, O. Jiménez Farías, A. Valdés-Hernández, P. H. Souto Ribeiro, L. Davidovich, and S. P. Walborn, Flow of quantum correlations from a two-qubit system to its environment, Phys. Rev. A **89**, 022339 (2014).
 - [42] P. G. Kwiat, E. Waks, A. G. White, I. Appelbaum, and P. H. Eberhard, Ultrabright source of polarization-entangled photons, Phys. Rev. A **60** R773 (1999).
 - [43] W. Dür and J. Cirac, Phys. Rev. A **61**, 042314 (2000).
 - [44] O. Gühne and M. Seevinck, New J. Phys. **12**, 053002 (2010).
 - [45] S. Szalay, Phys. Rev. A **83**, 062337 (2011).
 - [46] B. Jungnitsch, T. Moroder, and O. Gühne, Phys. Rev. Lett. **106**, 190502 (2011).
 - [47] J. Gruca, W. Laskowski, M. Żukowski, N. Kiesel, W. Wic-zorek, C. Schmid, and H. Weinfurter, Phys. Rev. A **82**, 012118 (2010).
 - [48] J.-D. Bancal, N. Gisin, Y.-C. Liang, and S. Pironio, Phys. Rev. Lett. **106**, 250404 (2011).
 - [49] H.M. Wiseman, S.J. Jones and A.C. Doherty, Phys. Rev. Lett. **98**, 140402 (2007);
 - [50] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani and S. Wehner, Rev. Mod. Phys. **86**, 419 (2014).
 - [51] J. F. Sturm, Opt. Methods and Software, **11-12**, 625 (1999). M. Grant and S. Boyd. CVX: Matlab software for disciplined convex programming, version 2.1. <http://cvxr.com/cvx>, March 2014.
 - [52] M. Horodecki, P. Horodecki, R. Horodecki, Separability of mixed states: necessary and sufficient conditions, Phys. Lett. A **223**, 1 (1996).
 - [53] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Phys. Rev. Lett. **88**, 187904 (2002); Phys. Rev. A **69**, 022308 (2004).
 - [54] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Phys. Rev. A **71**, 032333 (2005).
 - [55] M.F. Pusey, Phys. Rev. A **88**, 032313 (2013).
 - [56] M. Navascués, G. de la Torre, and T. Vértesi, Phys. Rev. X **4**, 011011 (2014).
 - [57] M. Navascués, S. Pironio, and A. Acín, Phys. Rev. Lett. **98**, 10401 (2007); New J. Phys. **10**, 73013 (2008).
 - [58] O. Gühne and G. Tóth, Phys. Rep. **474**, 1 (2009).